Bundesinstitut für Risikobewertung

Anhang A Leistungsbeschreibung
Bereitstellung von Cloud Compute Services für BfR / KIDA

1. Einleitung

Der Auftraggeber plant die Beschaffung von Cloud Compute Ressourcen und Services, um im Rahmen des KIDA- (KI- und Daten-Akzelerator) -Projekts den Wissenschaftler:innen des Auftraggebers und der beteiligten KIDA-Einrichtungen Services im Bereich der Daten- und Modellnutzung anbieten zu können. Die folgende Leistungsbeschreibung definiert die Anforderungen an die Cloud Compute Ressourcen und Services.

2. Information zum Auftraggeber

Im Mittelpunkt der Arbeit des Auftraggebers steht der Mensch als Verbraucher. Mit seiner unabhängigen wissenschaftlichen Bewertung, Forschung und transparenten Kommunikation von Bewertungsergebnissen trägt das Institut maßgeblich dazu bei, dass Lebensmittel, Stoffe und Produkte sicherer werden. Zentrale Aufgabe des Auftraggebers ist die wissenschaftliche Risikobewertung von Lebens- und Futtermitteln sowie von Stoffen und Produkten als Grundlage des gesundheitlichen Verbraucherschutzes der Bundesregierung.

3. Gegenstand der Ausschreibung (Scope)

Für die Bereitstellung von Services im Bereich der Daten- und Modellnutzung des KIDA-Projekts gibt es mehrere Anwendungsfälle. Zum einen plant der Auftraggeber einen Service anzubieten, in dem fertig trainierte KI-Modelle im sogenannten FSKX-Format über ein Repositorium bereitgestellt und bei Bedarf mit Nutzer-definierten Eingaben in einer Container-basierten Umgebung ausgeführt werden können. Zudem soll eine Graph-Datenbank bereitgestellt werden, in der sogenannte „Linked Data“ zum Austausch der Forschenden untereinander bereitgestellt werden. Außerdem sollen KI-gestützte Services und Softwareanwendungen bereitgestellt werden, die die Erstellung von FSKX-formatierten Modellen und von Linked Data ermöglichen.

Gegenstand der Ausschreibung ist die Lieferung von Cloud-Leistungen auf einer effizienten und kostengünstigen Cloud Plattform insbesondere aus den Kategorien IaaS, PaaS und MCS, sowie der Betrieb der Plattform. Folgende IT-Servicegruppen sind dabei im Minimum zu bedienen:

- Server

- Storage
- Netzwerk
- Container und Kubernetes Services
- Sicherheit inkl. IAM, Zertifikat und Key Management
- Kostenmanagementservices

Da einige der zu berechnenden Modelle eine hohe Komplexität haben und entsprechend viel Rechenleistung benötigen, werden auch GPU-Ressourcen vom Auftraggeber bereitgestellt. Die ausgeschriebenen Cloud-Ressourcen werden über ein Kontingentmodell bereitgestellt.

4. Leistungsort und -zeitraum

Leistungsort	EU, Zugriff über das Internet
Laufzeit	3 Jahre nach Zuschlagserteilung (1x Verlängerungsoption von 12 Monaten)

5. Leistungsbeschreibung

5.1 Generelle Zielsetzung

Der Auftraggeber setzt Cloud Compute Services gezielt dazu ein, um innovative, anforderungsgerechte, sichere und wirtschaftliche Serviceangebote im Bereich der Daten- und Modellnutzung des KIDA 2.0 Projekts für die KIDA-Projektpartner sowie im Rahmen der RAKIP Initiative für die RAKIP Partner effizient und zeitnah erbringen zu können.

5.2 Bereitstellung der Cloud-Leistungen

Der Auftraggeber erwartet die Bereitstellung der spezifizierten Cloud Compute Services über automatisierte Verfahren auswählbar in einem Self Service Katalog. Die Bereitstellung der Dienste soll mit frei verfügbaren Prozeduren und Tools, wie z. B. Terraform, effizient unterstützt werden.

Die benötigten Cloud Compute Services beziehen sich im Wesentlichen auf IaaS- und PaaS-Services. Das schließt insbesondere auch die Nutzung von KI- oder IoT-Services in der Cloud ein.

Da der genaue Umfang der zukünftig benötigten Cloud Services zum jetzigen Zeitpunkt noch nicht festgelegt werden kann, sollen möglichst viele unterschiedliche Services abrufbar sein.

Um die Transparenz der genutzten Leistungen zu gewährleisten, ist eine Separierung der Leistungen in verschiedene Services, Accounts, und Mandanten für jeden Bereich möglich.

Für die Kostentransparenz und damit der Auftraggeber ggf. frühzeitig gegensteuern kann, muss eine zeitnahe Kostenkontrolle möglich sein. Dies kann z. B. mittels entsprechender Dashboards realisiert werden. Die Abrechnung erfolgt monatlich und basiert auf dem Verbrauch pro Service, pro Mandanten und pro Account. Damit soll sichergestellt werden, dass deaktivierte Systeme keine laufenden bzw. nur minimale Kosten verursachen. Die Bereitstellung dieser Kostenkontrolle ist Bestandteil des u. g. Grundkontingentes.

Die Cloud Computer Services werden derart gestaltet, dass es ermöglicht wird einen Cloud-Diensteanbieter zu wechseln oder den Cloud-Dienst bzw. die Daten in die eigene IT-Infrastruktur zurückzuholen.

Um die Einhaltung der geltenden Datenschutzgesetze zu gewährleisten, sind die Cloud-Services von Rechenzentren innerhalb der EU zu erbringen (Regionalisierung).

Es sind keine Projekte mit Daten mit erhöhtem Schutzbedarf vorgesehen. Vertrauliche Daten dürfen nicht auf die Cloud-Ressourcen eingebracht werden.

5.3 Beschreibung der geforderten Cloud Compute Services (A-Kriterien)

Die geforderten Cloud-Leistungen ergeben sich aus den geplanten Serviceangeboten im Bereich Daten- und Modellnutzung des KIDA und RAKIP-Projektes, die vom Auftraggeber zu erbringen sind.

Hinweis zur Angebotserstellung:
Bei den folgenden Kriterien handelt es sich um Ausschlusskriterien (A-Kriterien). Eine Nichterfüllung führt zum Ausschluss des Angebotes gemäß § 42 Abs. 1 Nr. 4 UVgO.

5.3.1 Leistungsgruppe Server

- Es wird eine mandantenfähige Plattform zur Bereitstellung von virtuellen Servern/Systemen betrieben.
- Es werden Instanzen von virtuellen Maschinen ohne GPU-Unterstützung auf Basis von Linux angeboten.
- Es werden Instanzen von virtuellen Maschinen mit GPU-Unterstützung auf Basis von Linux angeboten.
- Es werden mindestens drei verschiedene Instanzkategorien mit verschiedenen Schwerpunkten bezüglich der Rechen-, Speicher und Netzwerkleistung angeboten.
- Verschiedene Preismodelle werden für die Instanzen angeboten, mindestens jedoch Pay-per-Use und Reservierung (24/7 durchgehender Betrieb).
- Es ist möglich, die Instanztypen nachträglich hinsichtlich der Rechen-, Speicher- und Netzwerkleistung anzupassen.
- Es stehen dokumentierte Werkzeuge und/oder APIs zur Verwaltung der Instanzen zur Verfügung.
- Werkzeuge und/oder APIs zur automatischen Skalierung von Instanzen stehen zur Verfügung.
- Die Linux-Distributionen Ubuntu und SuSE Enterprise stehen als installierbares Betriebssystem zur Verfügung.
- Es gibt eine Management-Umgebung zur Kapazitätsplanung und Jobsteuerung der Computing-Ressourcen.
- Die Instanzen werden hinsichtlich Zuverlässigkeit, Verfügbarkeit und Performance überwacht.
- Sichere Anmeldeinformation werden für den Zugang zu den Instanzen verwendet. Die Sicherung der Anmeldeinformationen unterliegt einer ständigen Weiterentwicklung und beinhaltet im Minimum die Geheimhaltung von Authentifizierungsinformationen inklusive sicherer Anmeldeverfahren sowie im Folgenden:
    - Die Zuteilung geheimer Authentifizierungsinformationen (z. B. Passwörter, Zertifikate, Sicherheitstoken) an interne und externe Benutzer des Auftragnehmers oder des Auftraggebers erfolgt, soweit dies organisatorischen oder technischen

Verfahren des Auftragnehmers unterliegt, in einem geordneten Verfahren, das die Vertraulichkeit der Informationen sicherstellt.

- Soweit diese initial vergeben werden, sind diese nur temporär, höchstens aber 14 Tage gültig. Benutzer werden ferner gezwungen, diese bei der ersten Verwendung zu ändern.
- Der Zugriff des Auftragnehmers auf Authentifizierungsinformationen des Auftraggebers ist streng reglementiert, mit dem Auftraggeber kommuniziert und erfolgt nur, wenn es für die Aufgabenwahrnehmung notwendig ist („Need-to-know-Prinzip“). Die Zugriffe werden dokumentiert und dem Auftraggeber mitgeteilt.
- Die Vertraulichkeit der Anmeldeinformationen von internen und externen Benutzern unter Verantwortung des Auftragnehmers sind durch die folgenden Maßnahmen geschützt:
  - Identitätsprüfung durch vertrauenswürdige Verfahren;
  - Verwendung anerkannter Industriestandards zur Authentifizierung und Autorisierung (z. B. Multi- Faktor-Authentifizierung, keine Verwendung von gemeinsam genutzten Authentifizierungsinformationen, automatischer Ablauf).
  - Multi-Faktor-Authentifizierung für Administratoren des Auftragnehmers (z. B. durch Smart Card oder biometrische Merkmale) ist zwingend erforderlich.

- Die virtuellen Instanzen haben die Möglichkeit verschiedene Storage Klassen anzubinden.
- Es gibt die Möglichkeit, auf den virtuellen Maschinen Open-Source-, proprietäre und Individualsoftware zu installieren und auszuführen.

5.3.2 Leistungsgruppe Netzwerk

- Es gibt eine DNS-Verwaltung, die Ipv4 und Ipv6 kompatibel ist.
- Mechanismen gegen Angriffe wie Distributed Denial of Service (DdoS) werden angeboten.
- Load Balancer Services werden angeboten.
- Es werden öffentliche Ipv4 und Ipv6 Adressen angeboten.
- Es werden VPC – Virtual Private Cloud Netzwerkumgebungen angeboten.

5.3.3 Leistungsgruppe Speicher

- Blockspeicher zur Verwendung von E/A-intensiven Lese-/Schreibvorgänge wird angeboten.
- Es wird Objektspeicher zur Verwendung von Inhaltsverteilung, Sicherung, Archivierung, Notfallwiederherstellung angeboten.

5.3.4 Leistungsgruppe PaaS

- Eine Container-Registry kann bereitgestellt werden.
- Managed Container-Services (Kubernetes) werden angeboten.
- Tools zur Überwachung der Containerumgebung werden angeboten.

- Serverless Containerumgebungen können bereitgestellt werden.

5.3.5 Leistungsgruppe Cloud Service Provider/Reseller

- Der Auftragnehmer ist in dem Partnerprogramm des jeweilig angebotenen Cloudanbieter registriert, sofern er nicht selber als Cloudanbieter auftritt.
- Ein Compliance-Programm wird nachgewiesen und unterstützt in folgenden Bereichen:
  - Continuous Auditing
  - Compliance: Monitoring gesetzlicher Vorschriften und Auflagen
  - Fraud: Überwachung der Zugriffsrechte und der Segregation of Duties (SoD)
  - Corporate Policy Enforcement: Überwachung der Einhaltung von Konzern- und Unternehmensrichtlinien
  - Datenschutz: Überwachung des Zugriffs auf private und sensible Informationen, wie z. B. Mitarbeiter- oder Kundendaten
- Nachweise für die Umsetzung anerkannter Standards für IT-Service-Management. Dies umfasst Unterstützung der Geschäftsprozesse durch IT-Service Management (ITSM) nach ISO 20000 oder ITIL.
- Möglichkeit einer konsolidierten Rechnung über die unterschiedlichen Cloud-Services wird angeboten. Die Umsetzung von Tagging-Strategien (z. B. nach Kostenstellen, Projekten) wird unterstützt.
- Tools zur Unterstützung des Kostenmanagements und der Zuordnung von Kosten zu dem Verursacher werden angeboten.
- Gesetze zur Steigerung der Energieeffizienz in Deutschland (z.B. Energieeffizienzgesetz - EnEfG Ausfertigungsdatum: 13.11.2023) werden eingehalten.
- Für alle Leistungen werden end to end Service-Level-Agreements (SLA) auf Basis des EVB-IT-Cloud-Vertrags angeboten.
- Der Support wird auf Deutsch und Englisch angeboten.

5.3.6 Leistungsgruppe IT-Service Management

- Der Auftragnehmer gibt seine Markterfahrung mit Cloud-Lösungen des jeweiligen Cloudanbieter mit Nennung von Kundenreferenzen an.
- Es gibt eine Überwachungsumgebung für die Überwachung von Leistung, Kosten und Sicherheit.
- Das System wird zur Erkennung von Anomalien überwacht.

5.3.7 Leistungsgruppe Datenschutz

- Der Schutz personenbezogener Daten in einer Cloud-Umgebung ist gewährleistet und die dazu definierten technischen und organisatorischen Maßnahmen werden eingehalten.
- Nachweise gemäß dem Schutz personenbezogener Daten durch die Erfüllung eines Standards wie die ISO/IEC 27018 oder andere liegen vor.
- Die Bereitstellung (Standort der Datenverarbeitungssysteme) der Cloud-Services erfolgt innerhalb der EU.

- Der administrative Betrieb der Cloud-Services wird nur von Mitarbeitenden innerhalb der EU durchgeführt.
- Die Cloud-Services bieten durchgängige Datenverschlüsselungsmöglichkeiten.
- Es ist ein Cloud-Services Zugriffsverwaltung (Identity- and Access Management) implementiert, was Berechtigungskonzepte auf Basis von Benutzer, Gruppen und Rollen unterstützt.

5.3.8 Leistungsgruppe Informationssicherheit

- Für den Geltungsbereich der bereitgestellten Cloud-Services wurde ein Unternehmensstandard für Informationssicherheit festgelegt.
- Die Plattform für die Cloud-Services gewährleistet eine Mandantenfähigkeit mit sicherer Trennung.

5.3.9 Leistungsgruppe IT-Sicherheit

- Es werden Firewall-Services angeboten.
- Eine Multifaktor-Authentifizierung für den Zugang zur Cloudumgebung wird angeboten.

5.3.10 Leistungsgruppe Betrieb

- Der Betrieb der Lösung erfolgt durch den Auftragnehmer und wird als Managed Service bereitgestellt. Der Auftragnehmer übernimmt die folgenden Dienstleistungen als Bestandteil des u. g. Grundkontingentes:
    - Einrichten der Cloud-Infrastruktur
    - Monitoring und Maintenance des Systems, inklusive Kostenmanagements, Umsetzung von Sicherheitsupdates und ggf. Anpassung an geänderte Sicherheitsanforderungen
    - Das Incident-Management in Kooperation mit dem Auftraggeber
    - Single Point of contact inkl. technische Problembehebung für alle Anfragen in Zusammenhang mit dem System
- Die folgenden Dienstleistungen werden von dem Auftragnehmer übernommen und nach Abstimmung mit dem Auftraggeber nach Aufwand abgerechnet:
    - Erstellung eines Betriebshandbuches und Datenschutz-Konzeptes in Abstimmung mit dem Auftraggeber
    - Erstellung eines Sicherheitskonzeptes, basierend auf den sich aus dem IT-Grundschutz ergebenen Sicherheitsanforderungen, und Abstimmung desselben mit dem Auftraggeber

5.3.11 Grundkontingent

Das Grundkontingent umfasst fest definierte Leistungen, die kontinuierlich zur Verfügung gestellt und entsprechend abgerechnet werden. Weitere Leistungen können bei Bedarf darüber hinaus flexibel abgerufen, zusätzlich in Anspruch genommen und separat vergütet werden.

Das Grundkontingent umfasst:

- 500 GB Object Storage (durchgehend laufend)
- 300 GB Container Registry Storage (durchgehend laufend)

- 3 Instanzen a 4 CPU, 16 GB Memory und 30 GB Storage (durchgehend laufend)
- 1 Instanz a 4 CPU, 16 GB Memory und 100 GB Storage (durchgehend laufend)
- 1 Instanz a 8 CPU, 128 GB Memory, 2 TB Storage und mindestens 2× NVIDIA A100 80GB (100h pro Jahr)
- Dienstleistungen gem. Nr. 5.3.10 „Leistungsgruppe Betrieb“

Die Wahl der konkreten GPU bleibt dem Auftragnehmer überlassen.

5.4 Beschreibung der gewünschten Cloud Compute Services (B-Kriterien)

Hinweis für die Angebotserstellung:
Zusätzlich zu den in den Punkten 5.3 bis 5.3.11 genannten Anforderungen soll der Auftragnehmer die folgenden Dienstleistungen übernehmen. Die Erfüllung dieser Anforderungen ist optional, wird allerdings im Rahmen der Angebotswertung positiv berücksichtigt, siehe Wertungsmatrix, Anhang zu den Teilnahmebedingungen (Anlage der Vergabeunterlagen).

5.4.1 Leistungsgruppe Server

- Container Instanzen sind mit verschiedenen Rechen- und Speicherressourcen als Self-Service-Technologie verfügbar, eine Container-Virtualisierung wird angeboten.
- Es wird einer oder mehrere der folgenden virtuellen Server angeboten:
  - 8 vCPU/16 GB
  - 8 vCPU/64 GB
  - 16 vCPU/512 GB

5.4.2 Leistungsgruppe Netzwerk

- Die Managementfunktionen stehen via Konsole und/oder APIs zur Verfügung.

5.4.3 Leistungsgruppe Speicher

- Ein Datenbackup der gespeicherten Daten wird zur Verfügung gestellt.
- Eine Verschlüsselung von im Speicher ruhenden Daten wird angeboten.

5.4.4 Leistungsgruppe IT-Service Management

- Alle KPI und SLA sowie das verbrauchte Volumen werden regelmäßig an den Auftraggeber berichtet und können per API abgerufen werden.
- Audit und Compliance Reports
- Einrichten eines ggf. bestehenden Ticketsystems
- Die Administration des Systems, inklusive der Neuanlage von Benutzern, virtuellen Maschinen und Basis-Containern

6. Zeitplan

Meilenstein 1	2 Wochen nach Zuschlag: Vorstellung des technischen und des kommerziellen Ansprechpartners im Rahmen eines Auftaktgesprächs Benennung des Datenschutz- und des Informationssicherheitsbeauftragten des Unternehmens.
Meilenstein 2	1 Monat nach Zuschlag: Bereitstellung von mind. 3 Cloud Accounts
Meilenstein 3	2 Monate nach Zuschlag: Bereitstellung des Betriebshandbuchs, Datenschutzkonzepts und Sicherheitskonzepts nach BSI-Grundschutz

7. Weitere Voraussetzungen

7.1 Einhaltung der EVB-IT Cloud

Die EVB-IT Cloud inklusive deren AGB sind als Grundlage des Vertrages einzuhalten.

7.2 Mitwirkung des Auftraggebers

Die Nutzer des Auftraggebers greifen über ihre eigene Infrastruktur auf die angebotenen Cloud Leistungen zu.

Der Auftraggeber benennt zu jedem Projekt einen Ansprechpartner, der als zentraler Ansprechpunkt fungiert, um Kontakte herzustellen und notwendige Entscheidungen zu treffen oder vorzubereiten.

7.3 Währung

Die Abrechnung der Leistungen erfolgt ohne USt. in Euro. Damit entstehen keine Währungsumrechnungsrisiken.

7.4 Sprache

Die Vertragssprache ist deutsch. Darüber hinaus kann der Auftragnehmer inklusive der Problemannahme und -bearbeitung auch in Englisch kommunizieren.

7.5 Sicherheit

Die im C5-Bericht genannten korrespondierenden Kontrollen für Cloud-Kunden werden durch den Auftragnehmer durchgeführt. Die Nachweise und sonstige Berichte des Cloud-Diensteanbieters werden durch den Auftragnehmer ausgewertet. Die Nachweise dürfen dabei über den Nutzungszeitraum keine zeitlichen Lücken enthalten. Bei Unklarheiten aus der Auswertung muss der Auftragnehmer diesen nachgehen und seine Prüf- und Kontrollrechte wahrnehmen. Ebenso wird geprüft, ob der Geltungsbereich und Schutzbedarf die genutzten Cloud-Dienste erfasst. Die Nachweise, sonstige Berichte und Auswertungsergebnisse werden dem Auftraggeber regelmäßig vorgelegt.

7.6 Prüfung Leistungsfähigkeit

Der Auftragnehmer prüft quartalsweise die Leistungsfähigkeiten des Cloud-Diensteanbieters und des Cloud-Dienstes sowie der Netzverbindung zum Cloud-Diensteanbieter und beurteilt diese. Dabei wird insbesondere die Einhaltung der vertraglich zugesicherten SLAs (mindestens VK1 gemäß EVB-IT Cloudvertrag AGB Kapitel 8.) überprüft.

7.7 Technologieklausel

Die im Rahmen dieser Ausschreibung vereinbarten Leistungen unterliegen einer ständigen technischen Weiterentwicklung bzw. Wandel. Daher kann der Auftraggeber eine Erweiterung um Produkte oder Leistungen für die genannten Warengruppen fordern.

Für die neu angebotenen Produkte/Services hat der Auftraggeber hierbei das Recht die Preise und Konditionen im Sinne der Vorgaben und seiner Anforderungen umfangreich inklusive der Abfrage anderer Marktteilnehmer zu prüfen.

Weiterhin kann der Auftraggeber, im Sinne einer Innovationsregelung, jederzeit eine Anpassung der Produkte/Services in der jeweiligen Kategorie verlangen. Dies gilt auch in Fällen in denen neue Services/Technologien auf dem Markt verfügbar sind.

Die Technologieklausel gilt auch in den Fällen, in denen angebotene Produkte/Services aus unvorhergesehenen Gründen nicht mehr geliefert/nicht mehr bezogen werden können. Der Auftragnehmer weist dies bei Bedarf entsprechend nach. Der Auftraggeber hat in allen Fällen das alleinige Bestimmungsrecht, welche Ersatzleistung stattdessen geliefert wird. Die angebotenen Ersatzleistungen müssen mindestens den Leistungsmerkmalen der Vorgängerservices entsprechen. Der Auftraggeber prüft die Kompatibilität innerhalb seiner Umgebung und kann die angebotene Leistung weiterhin einfordern.

7.8 Nachhaltigkeit sowie Klima- und Umweltschutz

Der Auftraggeber ist den Nachhaltigkeitszielen der Bundesregierung verpflichtet. Das Maßnahmenprogramm Nachhaltigkeit ist dabei ein wichtiger Bestandteil der Deutschen Nachhaltigkeitsstrategie.

Der Staatssekretärsausschuss für nachhaltige Entwicklung hat am 22. Mai 2023 den Monitoringbericht 2021 beschlossen, der den Stand der Umsetzung des neuen Maßnahmenprogramms Nachhaltigkeit der Bundesregierung (MP N) aus demselben Jahr wiedergibt. Es umfasst zehn Maßnahmenbereiche. Für einen Zeitraum von vier Jahren sind dazu jeweils strenge Nachhaltigkeitsvorgaben vereinbart, die es umzusetzen gilt. Schließlich kommt der Bundesverwaltung in den verschiedenen Aspekten des Verwaltungshandelns wie Energie und Klima, Beschaffung von Produkten und Dienstleistungen, Veranstaltungen sowie Diversität eine Vorbildfunktion zu.

Für den Klima- und Umweltschutz steht das Ziel der stetigen Reduktion der CO^2 Bilanz im Mittelpunkt. Hierbei stellt der Auftragnehmer einen jährlichen Report über die CO^2 Bilanz der verwendeten Services zur Verfügung und unterstützt den Auftraggeber bei der Auswahl der nachhaltigen, umweltschonenden Services.